Network Working Group
Request for Comments: 1760
Category: Informational

N. Haller
Bellcore
February 1995

The S/KEY One-Time Password System

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document describes the S/KEY* One-Time Password system as released for public use by Bellcore and as described in reference [3]. A reference implementation and documentation are available by anonymous ftp from ftp.bellcore.com in the directories pub/nmh/...

Overview

One form of attack on computing system connected to the Internet is eavesdropping on network connections to obtain login id's and passwords of legitimate users. The captured login id and password are, at a later time, used gain access to the system. The S/KEY One-Time Password system is designed to counter this type of attack, called a replay attack.

With the S/KEY system, only a single use password ever crosses the network. The user's secret pass-phrase never crosses the network at any time, including during login or when executing other commands requiring authentication such as the UNIX commands passwd or su. Thus, it is not vulnerable to eavesdropping/replay attacks. Added security is provided by the property that no secret information need be stored on any system, including the host being protected.

The S/KEY system protects against external passive attacks against the authentication subsystem. It does not prevent a network eavesdropper from gaining access to private information, and does not provide protection against "inside jobs" or against active attacks where the potential intruder as able to intercept and modify the packet stream.

Introduction

There are two sides to the operation of the S/KEY one-time password system. On the client side, the appropriate one-time password must be generated. On the host side, the server must verify the one-time password and permit the secure changing of the user's secret pass-phrase.

An S/KEY system client passes the user's secret pass-phrase through multiple applications of a secure hash function to produce a one-time password. On each use, the number of applications is reduced by one. Thus a unique sequence of passwords is generated. The S/KEY system host verifies the one-time password by making one pass though the secure hash function and comparing the result with the previous one-time password. This technique was first suggested by Leslie Lamport [1].

Secure Hash Function

A secure hash function is a function that is easy to compute in the forward direction, but computationally infeasible to invert. The S/KEY system is based on the MD4 Message Digest algorithm designed by Ronald Rivest [2]. Since the S/KEY authentication system went into use, the MD5 Message Digest was released. We have chosen to continue to use MD4 due the large number of client programs that have been distributed. Some sites have generated functionally similar systems based on MD5. Clearly clients and hosts must use the same secure hash function to interoperate.

The S/KEY system one-time passwords are 64 bits in length. This is believed to be long enough to be secure and short enough to be manually entered (see below, Form of Passwords) when necessary.

The S/KEY system applies the secure hash function multiple times, producing a 64 bit final output. MD4 accepts an arbitrary number of bits as input and produces a 128 bit output. The S/KEY secure hash function consists of applying MD4 to a 64 bit input and folding the output of MD4 with exclusive or to produce a 64 bit output.

Generation of One-Time Passwords

This section describes the computation of the S/KEY one-time passwords. It consists of a preparatory step in which all inputs are combined, a generation step where the secure hash function is applied multiple times, and an output function where the 64 bit one-time

password is displayed in readable form.

The client's secret pass phrase may be of any length and should be more than eight characters. As the S/KEY secure hash function described above accepts a 64 bit input, a preparatory step is needed. In this step, the pass phrase is concatenated with a seed that is transmitted from the server in clear text. This non-secret seed allows a client to use the same secret pass phrase on multiple machines (using different seeds) and to safely recycle secret passwords by changing the seed. (For ease in parsing, the seed may not contain any blanks, and should consist of strictly alphanumeric characters.) The result of the concatenation is passed through MD4, and then reduced to 64 bits by exclusive-OR of the two 8-byte halves.

The following code fragment uses the MD4 implementation defined in RFC 1320 [2] and defines the preparatory step:

```
strcpy(buf,seed);
strcat(buf,passwd);
MDbegin(&md)
MDupdate(&md,(unsigned char *)buf,8*buflen);

/* Fold result to 64 bits */
md.buffer[0] ^= md.buffer[2];
md.buffer[1] ^= md.buffer[3];
```

A sequence of one-time passwords is produced by applying the secure hash function multiple times to the output of the preparatory step (called S). That is, the first one-time password is produced by passing S through the secure hash function a number of times (N) specified by the user. The next one-time password is generated by passing S though the secure hash function N-1 times. An eavesdropper who has monitored the transmission of a one-time password would not be able to generate any succeeding password because doing so would require inverting the hash function.

Form of Passwords

The one-time password generated by the above procedure is 64 bits in length. Entering a 64 bit number is a difficult and error prone process. Some S/KEY system one-time password calculator programs insert this password into the input stream, others make it available for system cut and paste. Some arrangements require the one-time password to be entered manually. The S/KEY system is designed to facilitate this manual entry without impeding automatic methods. The one-time password is therefore converted to, and accepted as, a sequence of six short (1 to 4 letter) English words. Each word is chosen from a dictionary of 2048 words; at 11 bits per word, all

one-time passwords may be encoded. Interoperability requires at all S/KEY system hosts and calculators use the same dictionary. The standard dictionary is attached to this RFC.

Verification of One-Time Passwords

A function on the host system that requires S/KEY authentication is expected to issue an S/KEY challenge. This challenge give the client the current S/KEY parameters - the sequence number and seed. It is important that the S/KEY challenge be in a standard format so that automated clients (see below) can recognize the challenge and extract the parameters. The format of the challenge is:

s/key sequence_integer seed

The three tokens are separated by single space characters. The challenge is terminated by a blank or a newline.

Given the parameters and the secret pass phrase, the client can compute (or lookup) the one time password. It then passes it to the host system where it can be verified.

The host system has a file (on the UNIX reference implementation it is /etc/skeykeys) containing, for each user, the one-time password from the last successful login, or it may be initialized with the first one-time password of the sequence using the keyinit command (this command name may be implementation dependent). To verify an authentication attempt, it passes the transmitted one-time password through the secure hash function one time. If the result of this operation matches the stored previous one-time password, the authentication is successful and the accepted one-time password is stored for future use.

Because the number of hash function applications executed by the client decreases by one each time, at some point the user must reinitialize the system of be unable to login again. This is done by using the keyinit command which allows the changing of the secret pass phrase, the iteration count, and the seed. A frequent technique is to increment a trailing digit(s) of the seed and to reset the iteration count (to something in range of 500-1000).

Clients

Several programs are available to calculate S/KEY one time passwords.

Included in the reference implementation are command line interfaces for UNIX and PC systems (key), TSR interfaces for PCs (ctkey, termkey, and popkey), and GUI interfaces for Macintosh and Windows (keyapp and un-named Macintosh interface).

The most basic calculator is the key command whose format is:

```
key [-n count] sequence seed
```

The optional count is used to display more than a single one time password. This is useful to create a paper list of one time passwords.

The most automated calculator is the termkey program that runs as a Terminate and Stay Resident (TSR) program on a PC. It scans the screen to find the S/KEY parameters, prompts for the secret pass phrase, and stuffs the one time password into the keyboard buffer.

Acknowledgements

The idea behind S/KEY authentication was first proposed by Leslie Lamport [1]. The specific system described was proposed by Phil Karn, who also wrote most of the reference implementation.

References

[1] Lamport, L., "Password Authentication with Insecure Communication", Communications of the ACM 24.11, November 1981, 770-772.

[2] Rivest, R., "The MD4 Message-Digest Algorithm", RFC 1320, MIT and RSA Data Security, Inc., April 1992

[3] Haller, N., "The S/KEY One-Time Password System", Proceedings of the ISOC Symposium on Network and Distributed System Security, February 1994, San Diego, CA

[4] Haller, N., and R. Atkinson, "On Internet Authentication", RFC 1704, Bell Communications Research and Naval Research Laboratory, October 1994

Security Considerations

This entire document is about Security Considerations.

Author's Address

Neil Haller
Bellcore
MRE 2Q-280
445 South Street
Morristown, NJ, 07960-6438, USA

Phone: +1 201 829-4478
Fax: +1 201 829-2504
EMail: nmh@bellcore.com

Dictionary for Converting Between S/KEY 6-Word and Binary Formats

This dictionary is from the module put.c. The code for this module, and an implementation of the entire S/KEY One Time Password System is available by anonymous ftp from ftp.bellcore.com in the directory pub/nmh/skey.

```
{       "A",    "ABE",  "ACE",  "ACT",  "AD",   "ADA",  "ADD",
"AGO",  "AID",  "AIM",  "AIR",  "ALL",  "ALP",  "AM",   "AMY",
"AN",   "ANA",  "AND",  "ANN",  "ANT",  "ANY",  "APE",  "APS",
"APT",  "ARC",  "ARE",  "ARK",  "ARM",  "ART",  "AS",   "ASH",
"ASK",  "AT",   "ATE",  "AUG",  "AUK",  "AVE",  "AWE",  "AWK",
"AWL",  "AWN",  "AX",   "AYE",  "BAD",  "BAG",  "BAH",  "BAM",
"BAN",  "BAR",  "BAT",  "BAY",  "BE",   "BED",  "BEE",  "BEG",
```

```
"BEN",   "BET",   "BEY",   "BIB",   "BID",   "BIG",   "BIN",   "BIT",
"BOB",   "BOG",   "BON",   "BOO",   "BOP",   "BOW",   "BOY",   "BUB",
"BUD",   "BUG",   "BUM",   "BUN",   "BUS",   "BUT",   "BUY",   "BY",
"BYE",   "CAB",   "CAL",   "CAM",   "CAN",   "CAP",   "CAR",   "CAT",
"CAW",   "COD",   "COG",   "COL",   "CON",   "COO",   "COP",   "COT",
"COW",   "COY",   "CRY",   "CUB",   "CUE",   "CUP",   "CUR",   "CUT",
"DAB",   "DAD",   "DAM",   "DAN",   "DAR",   "DAY",   "DEE",   "DEL",
"DEN",   "DES",   "DEW",   "DID",   "DIE",   "DIG",   "DIN",   "DIP",
"DO",    "DOE",   "DOG",   "DON",   "DOT",   "DOW",   "DRY",   "DUB",
"DUD",   "DUE",   "DUG",   "DUN",   "EAR",   "EAT",   "ED",    "EEL",
"EGG",   "EGO",   "ELI",   "ELK",   "ELM",   "ELY",   "EM",    "END",
"EST",   "ETC",   "EVA",   "EVE",   "EWE",   "EYE",   "FAD",   "FAN",
"FAR",   "FAT",   "FAY",   "FED",   "FEE",   "FEW",   "FIB",   "FIG",
"FIN",   "FIR",   "FIT",   "FLO",   "FLY",   "FOE",   "FOG",   "FOR",
"FRY",   "FUM",   "FUN",   "FUR",   "GAB",   "GAD",   "GAG",   "GAL",
"GAM",   "GAP",   "GAS",   "GAY",   "GEE",   "GEL",   "GEM",   "GET",
"GIG",   "GIL",   "GIN",   "GO",    "GOT",   "GUM",   "GUN",   "GUS",
"GUT",   "GUY",   "GYM",   "GYP",   "HA",    "HAD",   "HAL",   "HAM",
"HAN",   "HAP",   "HAS",   "HAT",   "HAW",   "HAY",   "HE",    "HEM",
"HEN",   "HER",   "HEW",   "HEY",   "HI",    "HID",   "HIM",   "HIP",
"HIS",   "HIT",   "HO",    "HOB",   "HOC",   "HOE",   "HOG",   "HOP",
"HOT",   "HOW",   "HUB",   "HUE",   "HUG",   "HUH",   "HUM",   "HUT",
"I",     "ICY",   "IDA",   "IF",    "IKE",   "ILL",   "INK",   "INN",
"IO",    "ION",   "IQ",    "IRA",   "IRE",   "IRK",   "IS",    "IT",
"ITS",   "IVY",   "JAB",   "JAG",   "JAM",   "JAN",   "JAR",   "JAW",
"JAY",   "JET",   "JIG",   "JIM",   "JO",    "JOB",   "JOE",   "JOG",
"JOT",   "JOY",   "JUG",   "JUT",   "KAY",   "KEG",   "KEN",   "KEY",
"KID",   "KIM",   "KIN",   "KIT",   "LA",    "LAB",   "LAC",   "LAD",
"LAG",   "LAM",   "LAP",   "LAW",   "LAY",   "LEA",   "LED",   "LEE",
"LEG",   "LEN",   "LEO",   "LET",   "LEW",   "LID",   "LIE",   "LIN",
"LIP",   "LIT",   "LO",    "LOB",   "LOG",   "LOP",   "LOS",   "LOT",
"LOU",   "LOW",   "LOY",   "LUG",   "LYE",   "MA",    "MAC",   "MAD",
"MAE",   "MAN",   "MAO",   "MAP",   "MAT",   "MAW",   "MAY",   "ME",
```



```
"MEG",   "MEL",   "MEN",   "MET",   "MEW",   "MID",   "MIN",   "MIT",
"MOB",   "MOD",   "MOE",   "MOO",   "MOP",   "MOS",   "MOT",   "MOW",
"MUD",   "MUG",   "MUM",   "MY",    "NAB",   "NAG",   "NAN",   "NAP",
"NAT",   "NAY",   "NE",    "NED",   "NEE",   "NET",   "NEW",   "NIB",
"NIL",   "NIP",   "NIT",   "NO",    "NOB",   "NOD",   "NON",   "NOR",
"NOT",   "NOV",   "NOW",   "NU",    "NUN",   "NUT",   "O",     "OAF",
"OAK",   "OAR",   "OAT",   "ODD",   "ODE",   "OF",    "OFF",   "OFT",
"OH",    "OIL",   "OK",    "OLD",   "ON",    "ONE",   "OR",    "ORB",
"ORE",   "ORR",   "OS",    "OTT",   "OUR",   "OUT",   "OVA",   "OW",
"OWE",   "OWL",   "OWN",   "OX",    "PA",    "PAD",   "PAL",   "PAM",
"PAN",   "PAP",   "PAR",   "PAT",   "PAW",   "PAY",   "PEA",   "PEG",
"PEN",   "PEP",   "PER",   "PET",   "PEW",   "PHI",   "PI",    "PIE",
"PIN",   "PIT",   "PLY",   "PO",    "POD",   "POE",   "POP",   "POT",
"POW",   "PRO",   "PRY",   "PUB",   "PUG",   "PUN",   "PUP",   "PUT",
"QUO",   "RAG",   "RAM",   "RAN",   "RAP",   "RAT",   "RAW",   "RAY",
"REB",   "RED",   "REP",   "RET",   "RIB",   "RID",   "RIG",   "RIM",
"RIO",   "RIP",   "ROB",   "ROD",   "ROE",   "RON",   "ROT",   "ROW",
"ROY",   "RUB",   "RUE",   "RUG",   "RUM",   "RUN",   "RYE",   "SAC",
"SAD",   "SAG",   "SAL",   "SAM",   "SAN",   "SAP",   "SAT",   "SAW",
"SAY",   "SEA",   "SEC",   "SEE",   "SEN",   "SET",   "SEW",   "SHE",
"SHY",   "SIN",   "SIP",   "SIR",   "SIS",   "SIT",   "SKI",   "SKY",
"SLY",   "SO",    "SOB",   "SOD",   "SON",   "SOP",   "SOW",   "SOY",
"SPA",   "SPY",   "SUB",   "SUD",   "SUE",   "SUM",   "SUN",   "SUP",
"TAB",   "TAD",   "TAG",   "TAN",   "TAP",   "TAR",   "TEA",   "TED",
"TEE",   "TEN",   "THE",   "THY",   "TIC",   "TIE",   "TIM",   "TIN",
"TIP",   "TO",    "TOE",   "TOG",   "TOM",   "TON",   "TOO",   "TOP",
"TOW",   "TOY",   "TRY",   "TUB",   "TUG",   "TUM",   "TUN",   "TWO",
"UN",    "UP",    "US",    "USE",   "VAN",   "VAT",   "VET",   "VIE",
"WAD",   "WAG",   "WAR",   "WAS",   "WAY",   "WE",    "WEB",   "WED",
"WEE",   "WET",   "WHO",   "WHY",   "WIN",   "WIT",   "WOK",   "WON",
"WOO",   "WOW",   "WRY",   "WU",    "YAM",   "YAP",   "YAW",   "YE",
"YEA",   "YES",   "YET",   "YOU",   "ABED",  "ABEL",  "ABET",  "ABLE",
"ABUT",  "ACHE",  "ACID",  "ACME",  "ACRE",  "ACTA",  "ACTS",  "ADAM",
"ADDS",  "ADEN",  "AFAR",  "AFRO",  "AGEE",  "AHEM",  "AHOY",  "AIDA",
"AIDE",  "AIDS",  "AIRY",  "AJAR",  "AKIN",  "ALAN",  "ALEC",  "ALGA",
```

```
"ALIA",  "ALLY",  "ALMA",  "ALOE",  "ALSO",  "ALTO",  "ALUM",  "ALVA",
"AMEN",  "AMES",  "AMID",  "AMMO",  "AMOK",  "AMOS",  "AMRA",  "ANDY",
"ANEW",  "ANNA",  "ANNE",  "ANTE",  "ANTI",  "AQUA",  "ARAB",  "ARCH",
"AREA",  "ARGO",  "ARID",  "ARMY",  "ARTS",  "ARTY",  "ASIA",  "ASKS",
"ATOM",  "AUNT",  "AURA",  "AUTO",  "AVER",  "AVID",  "AVIS",  "AVON",
"AVOW",  "AWAY",  "AWRY",  "BABE",  "BABY",  "BACH",  "BACK",  "BADE",
"BAIL",  "BAIT",  "BAKE",  "BALD",  "BALE",  "BALI",  "BALK",  "BALL",
"BALM",  "BAND",  "BANE",  "BANG",  "BANK",  "BARB",  "BARD",  "BARE",
"BARK",  "BARN",  "BARR",  "BASE",  "BASH",  "BASK",  "BASS",  "BATE",
"BATH",  "BAWD",  "BAWL",  "BEAD",  "BEAK",  "BEAM",  "BEAN",  "BEAR",
"BEAT",  "BEAU",  "BECK",  "BEEF",  "BEEN",  "BEER",  "BEET",  "BELA",
"BELL",  "BELT",  "BEND",  "BENT",  "BERG",  "BERN",  "BERT",  "BESS",
"BEST",  "BETA",  "BETH",  "BHOY",  "BIAS",  "BIDE",  "BIEN",  "BILE",
```



```
"BILK",  "BILL",  "BIND",  "BING",  "BIRD",  "BITE",  "BITS",  "BLAB",
"BLAT",  "BLED",  "BLEW",  "BLOB",  "BLOC",  "BLOT",  "BLOW",  "BLUE",
"BLUM",  "BLUR",  "BOAR",  "BOAT",  "BOCA",  "BOCK",  "BODE",  "BODY",
"BOGY",  "BOHR",  "BOIL",  "BOLD",  "BOLO",  "BOLT",  "BOMB",  "BONA",
"BOND",  "BONE",  "BONG",  "BONN",  "BONY",  "BOOK",  "BOOM",  "BOON",
"BOOT",  "BORE",  "BORG",  "BORN",  "BOSE",  "BOSS",  "BOTH",  "BOUT",
"BOWL",  "BOYD",  "BRAD",  "BRAE",  "BRAG",  "BRAN",  "BRAY",  "BRED",
"BREW",  "BRIG",  "BRIM",  "BROW",  "BUCK",  "BUDD",  "BUFF",  "BULB",
"BULK",  "BULL",  "BUNK",  "BUNT",  "BUOY",  "BURG",  "BURL",  "BURN",
"BURR",  "BURT",  "BURY",  "BUSH",  "BUSS",  "BUST",  "BUSY",  "BYTE",
"CADY",  "CAFE",  "CAGE",  "CAIN",  "CAKE",  "CALF",  "CALL",  "CALM",
"CAME",  "CANE",  "CANT",  "CARD",  "CARE",  "CARL",  "CARR",  "CART",
"CASE",  "CASH",  "CASK",  "CAST",  "CAVE",  "CEIL",  "CELL",  "CENT",
"CERN",  "CHAD",  "CHAR",  "CHAT",  "CHAW",  "CHEF",  "CHEN",  "CHEW",
"CHIC",  "CHIN",  "CHOU",  "CHOW",  "CHUB",  "CHUG",  "CHUM",  "CITE",
"CITY",  "CLAD",  "CLAM",  "CLAN",  "CLAW",  "CLAY",  "CLOD",  "CLOG",
"CLOT",  "CLUB",  "CLUE",  "COAL",  "COAT",  "COCA",  "COCK",  "COCO",
"CODA",  "CODE",  "CODY",  "COED",  "COIL",  "COIN",  "COKE",  "COLA",
"COLD",  "COLT",  "COMA",  "COMB",  "COME",  "COOK",  "COOL",  "COON",
"COOT",  "CORD",  "CORE",  "CORK",  "CORN",  "COST",  "COVE",  "COWL",
"CRAB",  "CRAG",  "CRAM",  "CRAY",  "CREW",  "CRIB",  "CROW",  "CRUD",
"CUBA",  "CUBE",  "CUFF",  "CULL",  "CULT",  "CUNY",  "CURB",  "CURD",
"CURE",  "CURL",  "CURT",  "CUTS",  "DADE",  "DALE",  "DAME",  "DANA",
"DANE",  "DANG",  "DANK",  "DARE",  "DARK",  "DARN",  "DART",  "DASH",
"DATA",  "DATE",  "DAVE",  "DAVY",  "DAWN",  "DAYS",  "DEAD",  "DEAF",
"DEAL",  "DEAN",  "DEAR",  "DEBT",  "DECK",  "DEED",  "DEEM",  "DEER",
"DEFT",  "DEFY",  "DELL",  "DENT",  "DENY",  "DESK",  "DIAL",  "DICE",
"DIED",  "DIET",  "DIME",  "DINE",  "DING",  "DINT",  "DIRE",  "DIRT",
"DISC",  "DISH",  "DISK",  "DIVE",  "DOCK",  "DOES",  "DOLE",  "DOLL",
"DOLT",  "DOME",  "DONE",  "DOOM",  "DOOR",  "DORA",  "DOSE",  "DOTE",
"DOUG",  "DOUR",  "DOVE",  "DOWN",  "DRAB",  "DRAG",  "DRAM",  "DRAW",
"DREW",  "DRUB",  "DRUG",  "DRUM",  "DUAL",  "DUCK",  "DUCT",  "DUEL",
"DUET",  "DUKE",  "DULL",  "DUMB",  "DUNE",  "DUNK",  "DUSK",  "DUST",
"DUTY",  "EACH",  "EARL",  "EARN",  "EASE",  "EAST",  "EASY",  "EBEN",
"ECHO",  "EDDY",  "EDEN",  "EDGE",  "EDGY",  "EDIT",  "EDNA",  "EGAN",
"ELAN",  "ELBA",  "ELLA",  "ELSE",  "EMIL",  "EMIT",  "EMMA",  "ENDS",
"ERIC",  "EROS",  "EVEN",  "EVER",  "EVIL",  "EYED",  "FACE",  "FACT",
"FADE",  "FAIL",  "FAIN",  "FAIR",  "FAKE",  "FALL",  "FAME",  "FANG",
"FARM",  "FAST",  "FATE",  "FAWN",  "FEAR",  "FEAT",  "FEED",  "FEEL",
"FEET",  "FELL",  "FELT",  "FEND",  "FERN",  "FEST",  "FEUD",  "FIEF",
"FIGS",  "FILE",  "FILL",  "FILM",  "FIND",  "FINE",  "FINK",  "FIRE",
"FIRM",  "FISH",  "FISK",  "FIST",  "FITS",  "FIVE",  "FLAG",  "FLAK",
"FLAM",  "FLAT",  "FLAW",  "FLEA",  "FLED",  "FLEW",  "FLIT",  "FLOC",
"FLOG",  "FLOW",  "FLUB",  "FLUE",  "FOAL",  "FOAM",  "FOGY",  "FOIL",
"FOLD",  "FOLK",  "FOND",  "FONT",  "FOOD",  "FOOL",  "FOOT",  "FORD",
"FORE",  "FORK",  "FORM",  "FORT",  "FOSS",  "FOUL",  "FOUR",  "FOWL",
"FRAU",  "FRAY",  "FRED",  "FREE",  "FRET",  "FREY",  "FROG",  "FROM",
"FUEL",  "FULL",  "FUME",  "FUND",  "FUNK",  "FURY",  "FUSE",  "FUSS",
```

"GAFF", "GAGE", "GAIL", "GAIN", "GAIT", "GALA", "GALE", "GALL",
"GALT", "GAME", "GANG", "GARB", "GARY", "GASH", "GATE", "GAUL",
"GAUR", "GAVE", "GAWK", "GEAR", "GELD", "GENE", "GENT", "GERM",
"GETS", "GIBE", "GIFT", "GILD", "GILL", "GILT", "GINA", "GIRD",
"GIRL", "GIST", "GIVE", "GLAD", "GLEE", "GLEN", "GLIB", "GLOB",
"GLOM", "GLOW", "GLUE", "GLUM", "GLUT", "GOAD", "GOAL", "GOAT",
"GOER", "GOES", "GOLD", "GOLF", "GONE", "GONG", "GOOD", "GOOF",
"GORE", "GORY", "GOSH", "GOUT", "GOWN", "GRAB", "GRAD", "GRAY",
"GREG", "GREW", "GREY", "GRID", "GRIM", "GRIN", "GRIT", "GROW",
"GRUB", "GULF", "GULL", "GUNK", "GURU", "GUSH", "GUST", "GWEN",
"GWYN", "HAAG", "HAAS", "HACK", "HAIL", "HAIR", "HALE", "HALF",
"HALL", "HALO", "HALT", "HAND", "HANG", "HANK", "HANS", "HARD",
"HARK", "HARM", "HART", "HASH", "HAST", "HATE", "HATH", "HAUL",
"HAVE", "HAWK", "HAYS", "HEAD", "HEAL", "HEAR", "HEAT", "HEBE",
"HECK", "HEED", "HEEL", "HEFT", "HELD", "HELL", "HELM", "HERB",
"HERD", "HERE", "HERO", "HERS", "HESS", "HEWN", "HICK", "HIDE",
"HIGH", "HIKE", "HILL", "HILT", "HIND", "HINT", "HIRE", "HISS",
"HIVE", "HOBO", "HOCK", "HOFF", "HOLD", "HOLE", "HOLM", "HOLT",
"HOME", "HONE", "HONK", "HOOD", "HOOF", "HOOK", "HOOT", "HORN",
"HOSE", "HOST", "HOUR", "HOVE", "HOWE", "HOWL", "HOYT", "HUCK",
"HUED", "HUFF", "HUGE", "HUGH", "HUGO", "HULK", "HULL", "HUNK",
"HUNT", "HURD", "HURL", "HURT", "HUSH", "HYDE", "HYMN", "IBIS",
"ICON", "IDEA", "IDLE", "IFFY", "INCA", "INCH", "INTO", "IONS",
"IOTA", "IOWA", "IRIS", "IRMA", "IRON", "ISLE", "ITCH", "ITEM",
"IVAN", "JACK", "JADE", "JAIL", "JAKE", "JANE", "JAVA", "JEAN",
"JEFF", "JERK", "JESS", "JEST", "JIBE", "JILL", "JILT", "JIVE",
"JOAN", "JOBS", "JOCK", "JOEL", "JOEY", "JOHN", "JOIN", "JOKE",
"JOLT", "JOVE", "JUDD", "JUDE", "JUDO", "JUDY", "JUJU", "JUKE",
"JULY", "JUNE", "JUNK", "JUNO", "JURY", "JUST", "JUTE", "KAHN",
"KALE", "KANE", "KANT", "KARL", "KATE", "KEEL", "KEEN", "KENO",
"KENT", "KERN", "KERR", "KEYS", "KICK", "KILL", "KIND", "KING",
"KIRK", "KISS", "KITE", "KLAN", "KNEE", "KNEW", "KNIT", "KNOB",
"KNOT", "KNOW", "KOCH", "KONG", "KUDO", "KURD", "KURT", "KYLE",
"LACE", "LACK", "LACY", "LADY", "LAID", "LAIN", "LAIR", "LAKE",
"LAMB", "LAME", "LAND", "LANE", "LANG", "LARD", "LARK", "LASS",
"LAST", "LATE", "LAUD", "LAVA", "LAWN", "LAWS", "LAYS", "LEAD",
"LEAF", "LEAK", "LEAN", "LEAR", "LEEK", "LEER", "LEFT", "LEND",
"LENS", "LENT", "LEON", "LESK", "LESS", "LEST", "LETS", "LIAR",
"LICE", "LICK", "LIED", "LIEN", "LIES", "LIEU", "LIFE", "LIFT",
"LIKE", "LILA", "LILT", "LILY", "LIMA", "LIMB", "LIME", "LIND",
"LINE", "LINK", "LINT", "LION", "LISA", "LIST", "LIVE", "LOAD",
"LOAF", "LOAM", "LOAN", "LOCK", "LOFT", "LOGE", "LOIS", "LOLA",
"LONE", "LONG", "LOOK", "LOON", "LOOT", "LORD", "LORE", "LOSE",
"LOSS", "LOST", "LOUD", "LOVE", "LOWE", "LUCK", "LUCY", "LUGE",
"LUKE", "LULU", "LUND", "LUNG", "LURA", "LURE", "LURK", "LUSH",
"LUST", "LYLE", "LYNN", "LYON", "LYRA", "MACE", "MADE", "MAGI",
"MAID", "MAIL", "MAIN", "MAKE", "MALE", "MALI", "MALL", "MALT",
"MANA", "MANN", "MANY", "MARC", "MARE", "MARK", "MARS", "MART",

"MARY", "MASH", "MASK", "MASS", "MAST", "MATE", "MATH", "MAUL",
"MAYO", "MEAD", "MEAL", "MEAN", "MEAT", "MEEK", "MEET", "MELD",
"MELT", "MEMO", "MEND", "MENU", "MERT", "MESH", "MESS", "MICE",
"MIKE", "MILD", "MILE", "MILK", "MILL", "MILT", "MIMI", "MIND",
"MINE", "MINI", "MINK", "MINT", "MIRE", "MISS", "MIST", "MITE",
"MITT", "MOAN", "MOAT", "MOCK", "MODE", "MOLD", "MOLE", "MOLL",
"MOLT", "MONA", "MONK", "MONT", "MOOD", "MOON", "MOOR", "MOOT",
"MORE", "MORN", "MORT", "MOSS", "MOST", "MOTH", "MOVE", "MUCH",
"MUCK", "MUDD", "MUFF", "MULE", "MULL", "MURK", "MUSH", "MUST",
"MUTE", "MUTT", "MYRA", "MYTH", "NAGY", "NAIL", "NAIR", "NAME",
"NARY", "NASH", "NAVE", "NAVY", "NEAL", "NEAR", "NEAT", "NECK",
"NEED", "NEIL", "NELL", "NEON", "NERO", "NESS", "NEST", "NEWS",
"NEWT", "NIBS", "NICE", "NICK", "NILE", "NINA", "NINE", "NOAH",
"NODE", "NOEL", "NOLL", "NONE", "NOOK", "NOON", "NORM", "NOSE",
"NOTE", "NOUN", "NOVA", "NUDE", "NULL", "NUMB", "OATH", "OBEY",
"OBOE", "ODIN", "OHIO", "OILY", "OINT", "OKAY", "OLAF", "OLDY",
"OLGA", "OLIN", "OMAN", "OMEN", "OMIT", "ONCE", "ONES", "ONLY",

```
"ONTO",  "ONUS",  "ORAL",  "ORGY",  "OSLO",  "OTIS",  "OTTO",  "OUCH",
"OUST",  "OUTS",  "OVAL",  "OVEN",  "OVER",  "OWLY",  "OWNS",  "QUAD",
"QUIT",  "QUOD",  "RACE",  "RACK",  "RACY",  "RAFT",  "RAGE",  "RAID",
"RAIL",  "RAIN",  "RAKE",  "RANK",  "RANT",  "RARE",  "RASH",  "RATE",
"RAVE",  "RAYS",  "READ",  "REAL",  "REAM",  "REAR",  "RECK",  "REED",
"REEF",  "REEK",  "REEL",  "REID",  "REIN",  "RENA",  "REND",  "RENT",
"REST",  "RICE",  "RICH",  "RICK",  "RIDE",  "RIFT",  "RILL",  "RIME",
"RING",  "RINK",  "RISE",  "RISK",  "RITE",  "ROAD",  "ROAM",  "ROAR",
"ROBE",  "ROCK",  "RODE",  "ROIL",  "ROLL",  "ROME",  "ROOD",  "ROOF",
"ROOK",  "ROOM",  "ROOT",  "ROSA",  "ROSE",  "ROSS",  "ROSY",  "ROTH",
"ROUT",  "ROVE",  "ROWE",  "ROWS",  "RUBE",  "RUBY",  "RUDE",  "RUDY",
"RUIN",  "RULE",  "RUNG",  "RUNS",  "RUNT",  "RUSE",  "RUSH",  "RUSK",
"RUSS",  "RUST",  "RUTH",  "SACK",  "SAFE",  "SAGE",  "SAID",  "SAIL",
"SALE",  "SALK",  "SALT",  "SAME",  "SAND",  "SANE",  "SANG",  "SANK",
"SARA",  "SAUL",  "SAVE",  "SAYS",  "SCAN",  "SCAR",  "SCAT",  "SCOT",
"SEAL",  "SEAM",  "SEAR",  "SEAT",  "SEED",  "SEEK",  "SEEM",  "SEEN",
"SEES",  "SELF",  "SELL",  "SEND",  "SENT",  "SETS",  "SEWN",  "SHAG",
"SHAM",  "SHAW",  "SHAY",  "SHED",  "SHIM",  "SHIN",  "SHOD",  "SHOE",
"SHOT",  "SHOW",  "SHUN",  "SHUT",  "SICK",  "SIDE",  "SIFT",  "SIGH",
"SIGN",  "SILK",  "SILL",  "SILO",  "SILT",  "SINE",  "SING",  "SINK",
"SIRE",  "SITE",  "SITS",  "SITU",  "SKAT",  "SKEW",  "SKID",  "SKIM",
"SKIN",  "SKIT",  "SLAB",  "SLAM",  "SLAT",  "SLAY",  "SLED",  "SLEW",
"SLID",  "SLIM",  "SLIT",  "SLOB",  "SLOG",  "SLOT",  "SLOW",  "SLUG",
"SLUM",  "SLUR",  "SMOG",  "SMUG",  "SNAG",  "SNOB",  "SNOW",  "SNUB",
"SNUG",  "SOAK",  "SOAR",  "SOCK",  "SODA",  "SOFA",  "SOFT",  "SOIL",
"SOLD",  "SOME",  "SONG",  "SOON",  "SOOT",  "SORE",  "SORT",  "SOUL",
"SOUR",  "SOWN",  "STAB",  "STAG",  "STAN",  "STAR",  "STAY",  "STEM",
"STEW",  "STIR",  "STOW",  "STUB",  "STUN",  "SUCH",  "SUDS",  "SUIT",
"SULK",  "SUMS",  "SUNG",  "SUNK",  "SURE",  "SURF",  "SWAB",  "SWAG",
"SWAM",  "SWAN",  "SWAT",  "SWAY",  "SWIM",  "SWUM",  "TACK",  "TACT",
"TAIL",  "TAKE",  "TALE",  "TALK",  "TALL",  "TANK",  "TASK",  "TATE",
```



```
"TAUT",  "TEAL",  "TEAM",  "TEAR",  "TECH",  "TEEM",  "TEEN",  "TEET",
"TELL",  "TEND",  "TENT",  "TERM",  "TERN",  "TESS",  "TEST",  "THAN",
"THAT",  "THEE",  "THEM",  "THEN",  "THEY",  "THIN",  "THIS",  "THUD",
"THUG",  "TICK",  "TIDE",  "TIDY",  "TIED",  "TIER",  "TILE",  "TILL",
"TILT",  "TIME",  "TINA",  "TINE",  "TINT",  "TINY",  "TIRE",  "TOAD",
"TOGO",  "TOIL",  "TOLD",  "TOLL",  "TONE",  "TONG",  "TONY",  "TOOK",
"TOOL",  "TOOT",  "TORE",  "TORN",  "TOTE",  "TOUR",  "TOUT",  "TOWN",
"TRAG",  "TRAM",  "TRAY",  "TREE",  "TREK",  "TRIG",  "TRIM",  "TRIO",
"TROD",  "TROT",  "TROY",  "TRUE",  "TUBA",  "TUBE",  "TUCK",  "TUFT",
"TUNA",  "TUNE",  "TUNG",  "TURF",  "TURN",  "TUSK",  "TWIG",  "TWIN",
"TWIT",  "ULAN",  "UNIT",  "URGE",  "USED",  "USER",  "USES",  "UTAH",
"VAIL",  "VAIN",  "VALE",  "VARY",  "VASE",  "VAST",  "VEAL",  "VEDA",
"VEIL",  "VEIN",  "VEND",  "VENT",  "VERB",  "VERY",  "VETO",  "VICE",
"VIEW",  "VINE",  "VISE",  "VOID",  "VOLT",  "VOTE",  "WACK",  "WADE",
"WAGE",  "WAIL",  "WAIT",  "WAKE",  "WALE",  "WALK",  "WALL",  "WALT",
"WAND",  "WANE",  "WANG",  "WANT",  "WARD",  "WARM",  "WARN",  "WART",
"WASH",  "WAST",  "WATS",  "WATT",  "WAVE",  "WAVY",  "WAYS",  "WEAK",
"WEAL",  "WEAN",  "WEAR",  "WEED",  "WEEK",  "WEIR",  "WELD",  "WELL",
"WELT",  "WENT",  "WERE",  "WERT",  "WEST",  "WHAM",  "WHAT",  "WHEE",
"WHEN",  "WHET",  "WHOA",  "WHOM",  "WICK",  "WIFE",  "WILD",  "WILL",
"WIND",  "WINE",  "WING",  "WINK",  "WINO",  "WIRE",  "WISE",  "WISH",
"WITH",  "WOLF",  "WONT",  "WOOD",  "WOOL",  "WORD",  "WORE",  "WORK",
"WORM",  "WORN",  "WOVE",  "WRIT",  "WYNN",  "YALE",  "YANG",  "YANK",
"YARD",  "YARN",  "YAWL",  "YAWN",  "YEAH",  "YEAR",  "YELL",  "YOGA",
"YOKE"   };
```